ANÁLISIS DE LA SEGURIDAD DEL PROTOCOLO DE COMUNICACIONES CAN

Ing. Alejandro Fourcade, Mg Jorge Eterovic
Departamento de Ingeniería e Investigaciones Tecnológicas Universidad Nacional de La Matanza
Florencio Varela 1903 (B1754JEC), San Justo, (5411) 4480-8900

afourcade@unlam.edu.ar; eterovic@unlam.edu.ar

RESUMEN

Desde su concepción, el protocolo de comunicaciones CAN (Controller Area Network), trata de dar solución a la transmisión de datos en los exigentes entornos industriales. Creado por Bosch en 1986, ofrece una opción robusta y confiable, por lo cual se ha transformado en el estándar para la industria automotriz [1].

Su arquitectura está pensada para satisfacer eficientemente las necesidades operativas de un vehículo. Pero hoy, el automóvil tal como se lo conocía una década atrás, ya no existe. Sus mecanismos han sido invadidos por dispositivos digitales, sensores, actuadores y tiene hasta 80 ECUs (Engine Control Unit: Unidad de Control de Motor) comunicadas entre sí. A esta complejidad se ha sumado una aún mayor: estar conectado a Internet constantemente.

Como sucedió recientemente con algunos protocolos inalámbricos ante el advenimiento del Internet de las Cosas (IoT), pasar de un dominio cerrado a uno abierto conectado a la nube, propicia la aparición de amenazas, vulnerabilidades y brechas de seguridad.

Este cambio de escenario no estuvo en los planes en el momento de la concepción de la arquitectura, y en el caso de CAN termina transformándose en una bomba de tiempo. La diferencia entre los dos escenarios es que no tiene las mismas consecuencias un ataque informático a una heladera que a un camión de carga circulando por una autopista.

El principal problema es que algunas de las fortalezas del protocolo CAN, se transforman en limitaciones a la hora de adaptarse a entornos abiertos. Este dilema no es nuevo, pero como el riesgo es creciente, es de crucial importancia encontrar soluciones de seguridad.

Palabras Clave: *Seguridad de Datos. Protocolo CAN. Seguridad en Automóviles Conectados.*

CONTEXTO

Este proyecto de investigación se desarrolla en el marco de un Programa de Incentivos a Docentes Investigadores de la Secretaría de Políticas Universitarias (PROINCE) en el Departamento de Ingeniería e Investigaciones Tecnológicas de la Universidad Nacional de La Matanza.

El proyecto es financiado por el propio Departamento y es del tipo investigación aplicada. El mismo consiste en el desarrollo de un banco didáctico de ensayo de motores térmicos. Los trabajos de campo y relevamientos realizados aportaron información valiosa y sirvieron como base para el presente trabajo.

1. INTRODUCCIÓN

Los automóviles eran hasta hace unos años dispositivos casi exclusivamente electromecánicos, pero en las últimas décadas se ha incorporado masivamente la electrónica digital y ha tomado preponderancia y criticidad en su funcionamiento. También la Tecnología de la Información (IT) tiene un papel fundamental en los diseños automotrices.

El uso de la IT en los vehículos es cada vez mayor y sus objetivos eran brindar conectividad y confort. Si bien se han alcanzado estas metas y se han maximizado las prestaciones, no se han tenido en cuenta las amenazas y vulnerabilidades ante ataques externos que tiene todo dispositivo conectado a una red abierta como Internet.

Es muy importante la gestión de la seguridad en los sistemas de información. Uno de los principales factores a considera cuando se evalúan

los posibles daños que una intrusión maliciosa puede ocasionar, es el tipo y tiempo de respuesta del sistema.

Los automóviles son sistemas que reaccionan en tiempo real y una de las características del protocolo CAN es su respuesta rápida garantizada. Por eso el daño eventual ante un ataque al sistema de control de un automóvil es muy alto, teniendo en cuenta que, por ejemplo, la dirección, los frenos y el acelerador dejaron de tener control mecánico y pasaron a ser comandados electrónicamente.

Las ECU son las que leen los sensores y comandan los actuadores de un vehículo. En las primeras unidades que incluían esta tecnología había exclusivamente una ECU central, pero en los vehículos actuales se pueden encontrar hasta 80 de ellas conectadas a través de buses de diferentes jerarquías. Por ejemplo, el bus CAN destinado al sistema de confort, tiene menor prioridad y velocidad de respuesta que el que controla el airbag.

Este complejo sistema maneja actualmente casi todos los dispositivos de un automóvil, desde su dirección hasta los frenos, pasando por las trabas de las puertas, el tablero de instrumentos, las ópticas y hasta en algunos modelos, las bombas de agua y combustible. En muchos casos no existe una opción mecánica que prevalezca por sobre la electrónica. Si la ECU decide doblar a la derecha, el volante no puede evitar que esto suceda.

El periodista de la revista Forbes Andy Greenberg, pudo constatar que su acompañante podía habilitar o deshabilitar desde su notebook MacBook, los frenos de una camioneta Ford Escape de 1500 kg. de peso [2]. La situación descripta deja ver la gravedad de una intrusión al sistema.

En los años venideros este panorama se hará todavía más complejo, lo que lleva a los investigadores de la seguridad de la información como Eugene Kaspersky, ampliamente conocido por su software antivirus, a agregar al entorno automotriz dentro de los posibles objetivos de un ataque informático [3].

En el futuro tendremos nuevas formas de conectividad, como CAR TO CAR (C2C) o CAR TO INFRASTRUCTURE (C2I), lo que aumentará la integración de los vehículos a las redes de datos, por lo que las amenazas y vulnerabilidades expuestas son solo la punta del iceberg.

Varios trabajos han demostrado la posibilidad de atacar la estructura de datos de un automóvil con los métodos tradicionales (sniffing, spoofing) o generando mensajes falsos. El bus CAN puede accederse desde varios puntos de ingreso, directamente desde el puerto OBD2 (On Board Diagnostics) disponible debajo del tablero, o mediante “wire tapping”, o sea hackeando los conductores internos.

La primera opción de seguridad es el cifrado de los datos [4], no es de fácil aplicación por las características del protocolo CAN, como ser: la velocidad de transmisión, la latencia y su estructura multimaestro/multicast.

En el escenario descripto, las soluciones parecerían provenir del análisis estadístico de los mensajes que ocupan el bus. De esta forma es posible observar desviaciones con respecto a datos históricos y alertar así de una intrusión externa maliciosa. En este sentido se han expuesto trabajos sobre la detección de anomalías que corresponden tanto a problemas técnicos como a ataques a la seguridad. Los procedimientos que se utilizan incluyen análisis de frecuencias, análisis multivariado de series temporales [5] y los basados en la entropía de la información [6].

Gracias al Big Data están disponibles las grabaciones de miles de vehículos que alimentan una gran base de datos que describe modelos de comportamiento usuales. Con estos datos podrían establecerse patrones de comportamiento, cuyas desviaciones podrían ser analizadas para determinar su origen.

A partir de 2006, un nuevo protocolo llamado FlexRay [7] entró al mercado, con mayor ancho de banda (dos canales de 10 Mbps) y la posibilidad de cifrado. Si bien su implementación es más cara y todavía no es un estándar, demuestra el interés de las grandes fábricas de automóviles de migrar a un nuevo protocolo más seguro.

En base al panorama expuesto y al estado del arte, el proyecto de investigación propone el análisis de las amenazas y vulnerabilidades a los automóviles y la búsqueda de soluciones de seguridad para el parque automotor existente.

2. LÍNEAS DE INVESTIGACION Y DESARROLLO

Como sucede frecuentemente, en nuestro caso el interés por la detección de los problemas de

seguridad en el bus CAN fue un efecto colateral de los estudios e investigaciones realizadas en pos de obtener información de los diferentes dispositivos electrónicos y mecánicos de un automóvil.

El proyecto que propició el presente trabajo fue el de la construcción de un banco de pruebas de motores. Para fabricar un banco de ensayo normalmente se utilizan sensores y dispositivos auxiliares (frenos, sistemas de enfriamiento), pero en las ocasiones en que el dispositivo bajo ensayo conserva el sistema CAN, este puede ofrecer interesante información complementaria.

Se realizaron ensayos sobre algunos modelos de automóviles para estudiar los diferentes sistemas de información de un vehículo. Se decidió, luego de conocer las capacidades de los sistemas, trabajar con tableros de instrumentos, que generan y reciben tramas CAN y también con vehículos completos. Para esta tarea se utilizaron tableros de Volkswagen Suran, Volkswagen Polo, una camioneta Toyota Hilux y una Volkswagen Suran.

El primer paso fue contactar especialistas en electrónica automotriz para que aportaran sus experiencias y expandieran así los alcances de la investigación. Se realizaron varias reuniones con conclusiones sumamente interesantes:

- Crecimiento del equipamiento electrónico en los automóviles (principalmente los de alta gama).
- La complejidad y diversidad de implementaciones en vehículos.
- Los cambios en el perfil del especialista que debe resolver los nuevos problemas relacionados con el ambiente digital.
- Al participar de pruebas de conexión al bus CAN en automóviles, ayudaron a comprender la facilidad con que se ingresa, la variedad de herramientas informáticas que existe para ello y lo potencialmente peligroso que resultaría un acceso malicioso.

Una vez finalizados los relevamientos de campo se comenzó con la elección del dispositivo a ensayar. Era necesario que reciba, transmita y que además muestre los resultados en forma gráfica. En este punto la decisión era utilizar como dispositivo a una ECU o a un tablero de instrumentos. Se optó por el tablero, por ajustarse mejor a los requisitos expuestos.

Si bien existen implementaciones estándar de la mensajería CAN, la mayoría de los fabricantes utilizan, además, mensajes exclusivos. Por eso para establecer comunicación con el tablero, se utilizaron varios métodos, diferentes velocidades y diferentes combinaciones de mensajes.

Para contar con la flexibilidad necesaria para hacer estas pruebas, era necesario tener acceso directo a la trama CAN, tanto para leer como para generar mensajes. Se desarrolló para esa tarea una herramienta informática llamada “CAN Sniffer” que permite la lectura y grabación de mensajes CAN y la generación de tramas. Está basada en el MCP2515, un chip que hace de interfaz del CAN SPI y la plataforma Raspberry Pi (3 y Zero). Los dispositivos se probaron en entornos de maestro/ esclavo y de multimaestro con varias ECUs [8].

Una vez que se contó con la posibilidad de capturar mensajes se determinó el procedimiento para leer los mensajes de control de una herramienta especializada de diagnóstico automotriz especial para Volkswagen. De esa forma se pudo descifrar cómo establecía la comunicación con el tablero de instrumentos. Esto permitió determinar el método más eficiente para tratar de que el tablero reaccione a mensajes externos generado por nuestro dispositivo. Luego de probar varias formas, la más eficaz demostró ser el ataque por fuerza bruta aplicado de forma metódica. Se enviaron mensajes generados secuencialmente para luego analizar la reacción del tablero.

Se verificó también, que al cambiar el tablero por uno externamente idéntico, pero del modelo Polo, fue necesario realizar nuevamente todo el procedimiento de detección de mensajes.

Para la grabación y análisis de las tramas recibidas y generadas se utilizó una herramienta de código abierto llamada Wireshark en su versión para Raspbian (sistema operativo de Raspberry Pi)

En paralelo a las pruebas con el tablero, se realizaron ensayos con una Toyota Hilux y un Volkswagen Suran, para verificar que lo que sucedía en las pruebas de laboratorio, se repitiera en vehículos reales.

3. RESULTADOS OBTENIDOS/ESPERADOS

Luego de realizar los ensayos descriptos, los resultados fueron interesantes tanto desde el punto de vista de la lectura de lo que sucede con algunos dispositivos conectados al bus CAN como en lo que respecta a su reacción ante la generación de mensajes. Como se mencionó, si bien existen varios estándares de protocolo CAN (SAE J1708, SAE J1587 SAE J1939), los fabricantes implementan mensajería propietaria y diferentes variantes. Una de ellas es, por ejemplo, el protocolo UDS (Unified Diagnostic Service), un protocolo de capa 7, adaptación del KPW2000 en CAN. Es por eso que la tarea de tratar de encontrar un dispositivo que se comunique con todos los sistemas es casi imposible y explica a su vez la variedad de herramientas, para diferentes marcas y usos que se ofrecen en el mercado.

Dentro de los resultados obtenidos podrían citarse los obtenidos en el desarrollo de dispositivos para llevar a cabo la investigación. En el proceso hacer ingeniería inversa fue necesario desarrollar hardware y programarlo. Los lenguajes de programación utilizados fueron C++ de diferentes plataformas (Arduino, Raspberry, STM32) y Python sobre Raspbian. Los dispositivos desarrollados fueron:

- CAN Sniffer básico
- CAN Sniffer extendido
- Driver de Tablero
- Nodo de relevamiento remoto

En la Figura 1 se pueden ver el tablero con su driver y el Sniffer. Esto fue presentado funcionando en la feria Exproyecto 2019, en la UNLaM.

En cuanto a los resultados de la investigación propiamente dichos fueron, hasta el momento:

- Ingeniería inversa de implementación CAN (estándar y propietaria).
- Inyección de mensajes a tableros y vehículos que interfieren su funcionamiento maliciosamente.
- Lectura de parámetros del automóvil en tiempo real vía ODB2.
- Lectura de parámetros de un automóvil interviniendo su cableado interno.
- Transmisión inalámbrica al nodo de registro de datos operativos de un vehículo.
- La verificación de que la mayoría de los resultados obtenidos en el banco de pruebas, eran consistentes con vehículos reales.

Figura 1: Tablero y Sniffer

El objetivo principal era obtener datos e interactuar con entornos automotrices, pero una de las conclusiones adicionales fue que la seguridad de un vehículo de calle está en riesgo dada la facilidad para ingresar y atacar su lógica de control.

Otra de las conclusiones fue que la electrónica automotriz ya tenía latente estos riesgos, pero las nuevas tecnologías de vehículos "siempre conectados" le suman gravedad. Hace años que la seguridad en los vehículos está en discusión, pero hasta hace poco era necesario el contacto físico para realizar la intrusión. Hoy eso ha comenzado a cambiar. En el horizonte cercano vemos camiones autónomos sin chofer surcando las rutas, por eso es indispensable hacer más robusta la seguridad de los sistemas vehiculares.

Las metas por cumplir para garantizar la seguridad de los datos en sistemas tecnológicos, confidencialidad, integridad, autenticidad, disponibilidad y no repudio; están lejos de ser alcanzadas actualmente por cualquier dispositivo que basa su comunicación en el protocolo CAN [9].

Si bien la industria está trabajando en mitigar estos riesgos en los nuevos modelos, hay un parque automotor existente que está en riesgo. Esta necesidad abre una línea de investigación posible: el desarrollo de un dispositivo conectable al puerto ODB2 para detectar intrusiones maliciosas por comparación estadística. En caso de camiones o vehículos de flota también sería instalable en un bus específico. Por ejemplo, el que

controla el consumo de combustible, el airbag, la dirección o los frenos.

Atacar un dispositivo puede ser tan sencillo como bombardearlo con mensajes y generar lo que se conoce como denegación de servicio (Denial of Service), dejándolo fuera de servicio en forma temporal o definitiva.

Como ejemplo del resultado obtenido en el proceso de ingeniería inversa del tablero de instrumentos de un VW Vento, se puede apagar o encender el testigo del airbag. Si se envía al identificador 80 (0X050 hexadecimal) el dato 0X000001, si X=0 apaga y si X=1 prende. Si se envía al identificador 1136 (0X470) los datos (X0000000) para X=1 prende la luz de giro a la izquierda, X=2 la derecha, X=3 la baliza. Ese mismo identificador maneja la luz del baúl y la luz de batería.

Los códigos para realizar las funciones descriptas se obtuvieron haciendo un barrido de identificadores y enviando datos al azar. También se determinó que, por ejemplo, en el caso del velocímetro, medidor de RPM y de combustible, es necesario enviar una combinación de varias tramas.

En resumen, los resultados obtenidos evidencian una interesante línea de investigación para desarrollar dispositivos no invasivos que aumenten la seguridad de los vehículos.

4. FORMACIÓN DE RECURSOS HUMANOS

El equipo de trabajo de este proyecto está formado por un ingeniero mecánico, un ingeniero electrónico y un especialista en seguridad. Como se mencionó anteriormente, este trabajo se desarrolló en el marco del proyecto de investigación: “Desarrollo de un banco didáctico de ensayo de motores térmicos”.

El desarrollo del proyecto de investigación generó varias líneas de trabajo, de múltiples disciplinas. Dada la complejidad, fue necesaria la colaboración de varios expertos con amplia experiencia en la industria y la investigación académica, tanto en la parte de electrónica automotriz, como de bancos de prueba de motores y de seguridad de datos.

Uno de los miembros del equipo de investigación se encuentra desarrollando su trabajo de tesis de posgrado de la Maestría en Informática de la UNLaM titulada: “µFramework: marco de referencia para desarrollos de sistemas embebidos” y su tutor es el Mg. Jorge Eterovic, integrante del proyecto de investigación [10].

5. BIBLIOGRAFIA

[**1**] Protocolo de Comunicaciones CAN; http://www.bosch-semiconductors.com/en/ubk_semiconductors/ip_modules_3/produkttabelle_ip_modules/can_literature_1/can_literature.html. 2019.

[2] Greenberg A., Hackers Reveal Nasty New Car Attacks — with me behind the wheel, https://www.forbes.com/sites/leemathews. 2019.

[3] Kapersky E., Viruses coming aboard? - https://securelist.com. 2005.

[4] Weimerskirch A., Wolf M., Wollinger T., State of the art: embedding security in vehicles, *Horst-Gortz-Institute for IT Security, Ruhr-University Bochum, Universittatsstraße, 44780 Bochum, Germany.* 2007.

[5] Theissler A., Anomaly detection in recordings from in-vehicle networks, IT-Designers GmbH, Esslingen, Germany, 2014.

[6] Marchetti M., Stabili D., Guido A., Colajani M. Evaluation on anomaly detection for in-vehicle networks through information-theoretic algorithms, University of Modena and Reggio Emilia, Italy, 2015.

[7] Hartzell, S., Stubel C. Automobile CAN bus network security and vulnerability, University of Washington, Seattle, USA. 2018.

[8] Miller C., Valasek C. Car Hacking: for poories, http://illmatics.com/car_hacking_poories.pdf. 2018.

[9] Hoppe T., Kilz S., Security threats to automotive can networks – practical examples and selected short-term countermeasures, Otto von Guericke University of Magdeburg, Germany. 2010.

[**10**] Fourcade A., Eterovic J., Pérez A., Rodofile G., µFramework: marco de referencia para desarrollo de sistemas embebidos; CoNaIISI 2019; RIISIC-CONFEDI-UNLaM, San Justo. 2019.